Attorney's Docket No. 1032326-000168

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)

Jean-Sebastien Coron) Group Art Unit: 2135

Application No.: 09/937,397) Examiner: NIRAV B. PATEL

Filed: April 1, 2002) Appeal No.: ______________

For: COUNTERMEASURE METHOD IN AN ELECTRIC COMPONENT IMPLEMENTING AN ELLIPTICAL CURVE TYPE PUBLIC KEY CRYPTOGRAPHY ALGORITHM)

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated April 18, 2006 finally rejecting claims 1-15, which are reproduced as the Claims Appendix of this brief.

Charge the fee of $ 500 set forth in 37 C.F.R. § 41.20(b)(2) to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.17, and 41.20 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Table of Contents

I. Real Party in Interest

The present application is assigned to Gemplus, a French corporation.

II. Related Appeals and Interferences

There are no other known appeals, interferences or judicial proceedings which will affect, or be directly affected by, or have bearing on the Board's decision in this appeal.

III. Status of Claims

The application contains claims 1-15, all of which are pending and stand finally rejected. This appeal is directed to all finally rejected claims.

IV. Status of Amendments

There were no amendments filed subsequent to the final Office Action.

V. Summary of Claimed Subject Matter

The claimed subject matter is generally directed to public key cryptography that is based upon elliptical curves. More particularly, the claims recite a countermeasure that inhibits the ability of a hacker, or the like, to discover the private key of a user by observing multiple cryptographic operations that employ the key. Background information on public key cryptography based upon elliptical curves is set forth in the specification at pages 3-7, and the techniques for attacking this type of cryptographic operation are described at pages 7-11.

The claimed countermeasure protects against these types of attacks by introducing an element of randomness in at least one of the parameters that is employed during the cryptographic operation. In one embodiment of the countermeasure, a randomized value for the private key *d* is employed. In another embodiment, a randomized value is used for the calculation modulus *p*. In a third embodiment, at least one of the points *P,Q* on the curve that are used to calculate the keys is made random.

The application contains three independent claims, namely claims 1, 6 and 11. A mapping of each of these claims to the disclosure is set forth hereinafter:

1. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves in which a deciphering integer d' is calculated, using a private key d and a number of points n on an elliptical curve, such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d **(page 11, lines 6-10)**, by effecting the operation Q=d*P, where P is a point on the curve **(page 11, lines 11-15)**, said method including the following steps:

1) determining a security parameter s **(page 11, lines 17-18)**;

2) drawing a random number k between 0 and 2^s **(page 11, line 19)**;

3) calculating the integer d'=d+k*n **(page 11, line 20)**; and

4) calculating Q=d'*P **(page 11, line 21)**.

6. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves defined on a finite field GF(p), where p is a prime number, according to the equation $y^2=x^3+ax+b$ **(page 12, lines 8-11)** and where a random calculation modulus of the form p'=p*r, where r is a random integer, is used at each new execution of the algorithm **(page 12, lines 11-15)**, said method including the execution of a scalar multiplication operation according to the following steps:

1) determining a security parameter s **(page 12, lines 20-21)**;

2) drawing a random number r whose binary representation comprises s bits **(page 12, lines 22-23)**;

3) calculating p'=p*r **(page 12, line 24)**;

4) executing the scalar multiplication operation Q=d.P, where P is a point on a curve, and said operation is performed modulo p' **(page 12, lines 25-26)**; and

5) performing the reduction operation modulo p of the coordinates of the point Q **(page 12, lines 27-28)**.

11. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves in which a new deciphering key d' is calculated, using the private key d and a number of points n on an elliptical curve, such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by performing the operation Q=d*P, where P is a point on the curve to which a scalar multiplication algorithm is applied, said method comprising the following steps:

1) drawing a random point R on the curve **(page 13, line 21)**;

2) calculating P'=P+R **(page 13, line 22)**;

3) performing the scalar multiplication operation Q'=d.P' **(page 13, line 23)**;

4) performing the scalar multiplication operation S=d.R **(page 13, line 24)**; and

5) calculating Q=Q' – S **(page 13, line 25)**.

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents two grounds of rejection to be reviewed on this appeal:

1. Claims 1-15 stand rejected on the grounds of obviousness-type double patenting in view of claims 1-7 of U.S. Patent No. 6,914,986;

2. Claims 1-15 stand rejected under 35 U.S.C. § 103 as being unpatentable over an article by Jerome A. Solinas entitled "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves", in view of U.S. Patent No. 6,064,740 ("Curiger").

VII. Argument

A. Double Patenting Rejection

Claims 1-15 were rejected on the grounds of obviousness-type double patenting in view of claims 1-7 of U.S. Patent No. 6,914,986. The Office Action contends that the only difference between the pending claims and those of the issued patent is the recitation of "determining a security parameter s". The Action goes on to allege that it would have been obvious to determine a security parameter for the algorithm.

MPEP §804 states "any analysis employed in an obviousness-type double patenting rejection parallels the guidelines for analysis of a 35 U.S.C. §103 obviousness determination." One issue to be reviewed, therefore, is whether the final Office Action establishes a prima facie case of obviousness that meets the criteria set forth in MPEP §2143. This section of the Manual states that a prima facie case of obviousness requires that there be a suggestion or motivation "in the references themselves" to modify a reference's teachings. The double patenting rejection is based upon a bald conclusion of obviousness, without any support therefor. Specifically, despite an express acknowledgement of a distinction between the claims of the pending application and those of the '986 patent, the Office Action does not cite any reference, nor otherwise provide any evidence, to show that this distinction was even known in the prior art, let alone that it would be obvious to apply it to the claimed subject matter of the '986 patent. Hence, the rejection fails to identify any motivation to modify the reference that can be found in the prior art.

1. Claims 1-5

Another of the criteria for a prima facie case of obviousness is that the reference "must teach or suggest all of the claim limitations." The recitation of determining a security parameter is not the *only* difference between the pending claims and those of the issued patent. For instance, claim 1 recites the step of drawing a random number between 0 and 2^s. Thus, the security parameter establishes the range of numbers from which the random number can be selected. Even if one were to assume that it is obvious to determine a security parameter, *per se*, the Office Action has not shown that it would be obvious to use the security parameter for this purpose.

Claim 1 also recites the step of "calculating the integer d'=d+k*n", where *k* is the random number and *n* has been defined as the number of points of an elliptical curve. In contrast, claim 1 of the '986 patent recites "calculating an integer d' such that d'=d+r", where *r* is a random value with the same size as *d*. The Office Action has not shown where this difference is suggested in the prior art. For instance, where is there a teaching to multiply the random number by the number of points of an elliptical curve before adding the result to *d*?

2. Claims 6-10

Claims 6 and 11 recite other distinctive features. For instance, claim 6 recites the steps of calculating p'=p*r, where *p* is a prime number and *r* is a random number, and executing the scalar multiplication operation Q=d.P modulo p'. With reference to this latter step, the Office Action refers to step 3 of claim 1 in the '986 patent. That step is recited as Q'=d'.P, where d'= d+r. In other words, in claim 1 of the '986 patent, Q'=d.P + r.P. There is no reference to performing this operation according to any particular modulus, let alone the one recited in claim 6 of the present application.

3. Claims 11-15

Claim 11 recites the steps of calculating P'= P+R, where P is a point on the curve and *R* is a random point on the elliptical curve, performing the scalar multiplications Q'=d.P' and S=d.R, and calculating Q=Q'-S. In connection with the recitation P'=P+R, the Office Action refers to step of claim 1 in the '986 patent, i.e. d'=d+r. In claim 11 of the present application, both P and R are points on the elliptic curve. Claim 1 of the '986 patent does not state that its values for d and r are points on the curve.

With respect to claim 11's recitation that Q'=d.P', the Office Action refers to step 3 of claim 1 in the '986 patent, i.e. Q'=d'.P. These are not the same operation. In claim 11 of the present application, since P'=P+R, Q'=d.P + d.R. In claim 1 of the '986 patent, d'=d+r, so that Q'=d.P + r.P. As can be seen, the second terms of the respective equations are different.

As set forth above, the final Office Action does not meet the requirements for a prima facie case of obviousness under 35 U.S.C. §103. As such, it fails to establish a proper case for the double patenting rejection.

B. Rejection Under 35 U.S.C. § 103

Claims 1-15 were rejected under 35 USC § 103, on the grounds that they were considered to be unpatentable over the article by Jerome A. Solinas entitled "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves", in view of the Curiger et al patent (US 6,064,740). The pending claims are directed to countermeasures against attacks on cryptographic operations, particularly those which are based upon elliptical curves. These countermeasures are effected by introducing a measure of randomness to the operations, so that the same calculation is not carried out every time the cryptographic algorithm is executed. The claims recite that the randomness can be implemented with the private key *d*, the calculation modulus *p'*, and the point P on the curve to which the scalar multiplication operation is applied.

The Solinas article is directed to elliptic scalar multiplication operations. Other than a brief mention that public-key protocols are based on elliptic curves, the article does not address the field of cryptography. In particular, it does not describe countermeasures to guard against attacks on public key cryptographic systems. Rather, the focus of the Solinas article is making the scalar multiplication more *efficient*.

1. Claims 1-5

Since it does not address countermeasures against attacks, the Solinas article does not disclose the features recited in the pending claims. For example, claim 1 recites the steps of drawing a random number *k*, and calculating the integer d'=d+k*n, where *n* is the number of points on an elliptical curve. The Office Action asserts that the Solinas article teaches these claimed steps, citing pages 360 and 361, with specific reference to Algorithms 2 and 3. However, neither of these algorithms relates to the selection and use of *random numbers* in the calculation of Q=d.p (or Q=n.P in the nomenclature of the Solinas article). Nor is there any apparent reason why a person would employ random numbers in the context of the Solinas article. If one is seeking to produce a faster multiplication algorithm, what is to be gained by introducing random values into the calculation?

In Appellant's initial response to this rejection, the examiner was requested to identify where the Solinas article teaches the specific steps of (1) determining a security parameter *s*, (2) drawing a random number *k* between 0 and 2^s, and (3) calculating the integer d'=d+k*n, where *n* is the number of points on the elliptical curve, as recited in claim 1. In reply, the final Office Action merely asserts that Algorithm 2 on page 360 corresponds to the first three steps of claim 1. Appellant is at a loss to understand the basis for this assertion. It is not apparent what value in Algorithm 2 corresponds to the claimed security parameters, nor where the algorithm discloses that such a value is to be used as an exponent to determine the upper limit for the range from which a random value is chosen. Nor does the Office Action indicate what statement in Algorithm 2 corresponds to the claimed calculation d'=d+k*n.

The Curiger patent was cited for its disclosure of using a microprocessor core to perform modular calculations. However, the Curiger patent does not contain any teachings that overcome the differences between the subject matter of claim 1 and the Solinas article that are identified above. While the Curiger patent is concerned with attacks on cryptosystems, it is not directed to cryptosystems that are based upon elliptical curves. Rather, it deals with operations that are characteristic of Diffie-Hellman and RSA encryption techniques. See, for example, column 2, lines 1-8.

More significantly, the Curiger patent does not disclose the use of random numbers to modify one or more of the parameters of the encryption or decryption algorithm. Instead, its approach to countering attacks is to "normalize" the modular math calculations, so that the timing and power requirements of the calculations are the same, regardless of whether the bit being processed is a one or a zero. See column 3, lines 38-40. As such, it does not disclose the above-noted features of claim 1 that are missing from the Solinas article.

Accordingly, the subject matter of claim 1 is not rendered unpatentable by the Solinas article, whether considered by itself or in combination with the Curiger patent.

2. Claims 6-10

For similar reasons, independent claims 6 and 11 are likewise patentable over the teachings of these references. The final Office Action groups claims 1, 6 and 11 under a single statement of rejection. In making the rejection, it only refers to the recitations of claim 1. The Office Action does not recognize that independent claims 6 and 11 recite steps that are different from those recited in claim 1. As such, even if, for the sake of argument, it were to be assumed that claim 1 is not patentable over the cited references, the Office Action does not contain any showing that would justify the rejection of independent claims 6 and 11.

For instance, claim 6 recites the steps of drawing a random number *r*, calculating p'=p*r, and performing the scalar multiplication operation Q=d.P modulo p'. While the Solinas article discloses the general equation Q=n.P on page 361, it does not disclose that this calculation is performed with respect to a modulus, let alone one that is based upon a random number.

3. Claims 11-15

Claim 11 recites the steps of drawing a random point *R* on the elliptical curve, calculating P'= P+R, performing the scalar multiplications Q'=d.P' and S=d.R, and calculating Q=Q'-S. It is noted that the Office Action does not address any of these claimed steps in the rejection of the claims. Nor is it apparent how the Solinas article could be interpreted to disclose them. As such, the Office Action has not established a *prima facie* case of obviousness upon which a proper rejection can be based, since it has not shown that all of the claimed limitations are taught or suggested in the prior art references.

C. Conclusion

For at least the foregoing reasons, the final Office Action fails to establish a prima facie case of obviousness, for either of the grounds of rejection set forth therein. The double patenting rejection is based upon an unsupported conclusion of obviousness, and does not identify where a number of elements of the currently pending claims are found in the claims of the '986 patent. The rejection under 35

U.S.C. §103 fails to show where a number of the features recited in the claims can be found in the references, despite Appellant's explicit request for such a showing.

The rejections are not properly founded in the statute or relevant case law, and should be reversed.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

(none)

X. Related Proceedings Appendix

(none)

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date January 29, 2007

By: James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves in which a deciphering integer d' is calculated, using a private key d and a number of points n on an elliptical curve, such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d’, gives the same result as with d, by effecting the operation Q=d*P, where P is a point on the curve, said method including the following steps:

1) determining a security parameter s;
2) drawing a random number k between 0 and 2^s;
3) calculating the integer d’=d+k*n; and
4) calculating Q=d'*P.

2. A countermeasure method according to Claim 1, wherein a new deciphering integer d’ is calculated at each new execution of the deciphering algorithm.

3. A countermeasure method according to Claim 1, further including the step of incrementing a counter at each new execution of the deciphering algorithm until a fixed value T is reached.

4. A countermeasure method according to Claim 3, wherein, once the value T has been reached, a new deciphering integer is calculated and the counter is reset to zero.

5. A countermeasure method according to Claim 3, wherein the value T is equal to the integer 16.

6. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves defined on a finite field GF(p), where p is a prime number, according to the equation $y^2=x^3+ax+b$ and where a random calculation modulus of the form p'=p*r, where r is a random

integer, is used at each new execution of the algorithm, said method including the execution of a scalar multiplication operation according to the following steps:

1) determining a security parameter s;
2) drawing a random number r whose binary representation comprises s bits;
3) calculating p'=p*r;
4) executing the scalar multiplication operation Q=d.P, where P is a point on a curve, and said operation is performed modulo p'; and
5) performing the reduction operation modulo p of the coordinates of the point Q.

7. A countermeasure method according to Claim 6, wherein a new integer is calculated at each new execution of the cryptography algorithm.

8. A countermeasure method according to Claim 6, further including the step of incrementing a counter at each new execution of the cryptography algorithm.

9. A countermeasure method according to Claim 8, wherein the counter is reset to zero when it has reached a value T.

10. A countermeasure method according to Claim 9, wherein the value T is equal to sixteen.

11. A countermeasure method in an electronic component implementing a public key cryptography algorithm based on the use of elliptical curves in which a new deciphering key d' is calculated, using the private key d and a number of points n on an elliptical curve, such that the deciphering of any enciphered message, by means of a deciphering algorithm, with d', gives the same result as with d, by performing the operation Q=d*P, where P is a point on the curve to which a scalar multiplication algorithm is applied, said method comprising the following steps:

1) drawing a random point R on the curve;
2) calculating P'=P+R;
3) performing the scalar multiplication operation Q'=d.P';
4) performing the scalar multiplication operation S=d.R; and
5) calculating Q=Q' – S.

12. A countermeasure method according to Claim 11, further including the step of incrementing a counter at each new execution of the deciphering algorithm up to a value T.

13. A countermeasure method according to Claim 12, wherein the counter is reset to zero once the value T has been reached.

14. A countermeasure method according to Claim 11, wherein the elliptical curve has two points such that S=d*R, and wherein steps 1 and 4 are replaced by the following steps 1' and 4':

1') Replacing R with 2.R.

4') Replacing S with 2.S.

15. A countermeasure method according to Claim 14, further including the step of incrementing a counter at each new execution of the deciphering algorithm up to a value T.